DIT

Telecommunications and Network Management

State User Gateway-to-Gateway Service Process

By

Chris Fellows

Wednesday, April 14, 2004

Table Of Contents

State User Gateway-to-Gateway Service Process

Date:	April, 27 2005
To:	Telecommunication Services
Priority:	1
Effective Date:	April, 2004
Training Time:	N/A
Related Documents:	DIT-TS 310-001 – Local Government Extranet (LGNET) Operations Guidelines
Issuing Department:	Telecommunication Services
Author(s):	Christopher Fellows – 517-241-1786
Document Owner:	Christopher Kar – 517-241-3460
Revision Number:	1.0

NOTE: See Revision History for Detailed Information on Tracking and Changes.

Revision History

Revision	Date	Author	Comments
1.0	04/03/04	C. Fellows	First draft of the template
1.1	04/9/04	C. Fellows	Added several Step-by-Step procedures
1.2	04/14/04	C. Fellows	Final Draft
1.3	04/27/05	C. Fellows	Update

Team Members

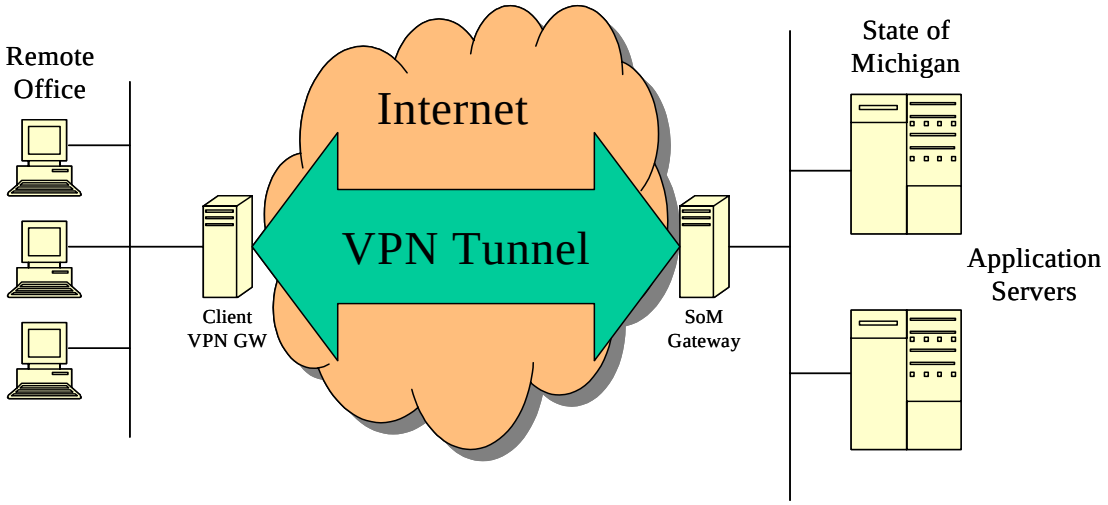
Name	Department	Contribution	Contact Information
Chris Fellows	Network Operations	VPN Specialist	517-241-1786
Mary Wenson	Network Operations	Network Support	517-241-7072
Douglas Sitterson	Network Operations	Security Specialist	517-241-7380
Alex Park	Network Operations	Extranet Specialist	517-373-0294
Tom Glomski	Enterprise Security	Risk Assessment	517-241-7067
Joe Sonefeld	Telephone Service Center	Financial Services	517-373-8624

Service Overview

The User Gateway-to-Gateway VPN service (User GW-to-GW) and Vendor Gateway-to-Gateway VPN service (Vendor GW-to-GW) is provided as a low cost alternative to traditional leased line connections to remote offices. This service can provide secure broadband communications between remote offices and the central State of Michigan (SoM) networks. It must be noted here and cannot be stressed enough, that **all VPN services depend on the public Internet and CAN NOT be guaranteed in any manner.** Service is provided on a "Best Effort" basis and recovery times from outages are susceptible to influences outside the control of the SoM and DIT Telecom.

The basic concept of this service takes advantage of the IPSEC standard for data encryption across public networks. DIT provides the hardware, software, (in the case of User GW-to-GW) and supports services to enable remote offices to securely communicate with the SoM core network over the public Internet. Users at the client end have a very similar experience as directly connected network users and can access most SoM applications such as DCDS, GroupWise, HRMN, and Remedy. Vendor's can be granted permission to access systems that they support over this service. The Following illustration depicts the basic network diagram for a typical GW-to-GW connection

Basic Network Diagram of Gateway-to-Gateway VPN



Here are a few things to keep in mind when considering this service

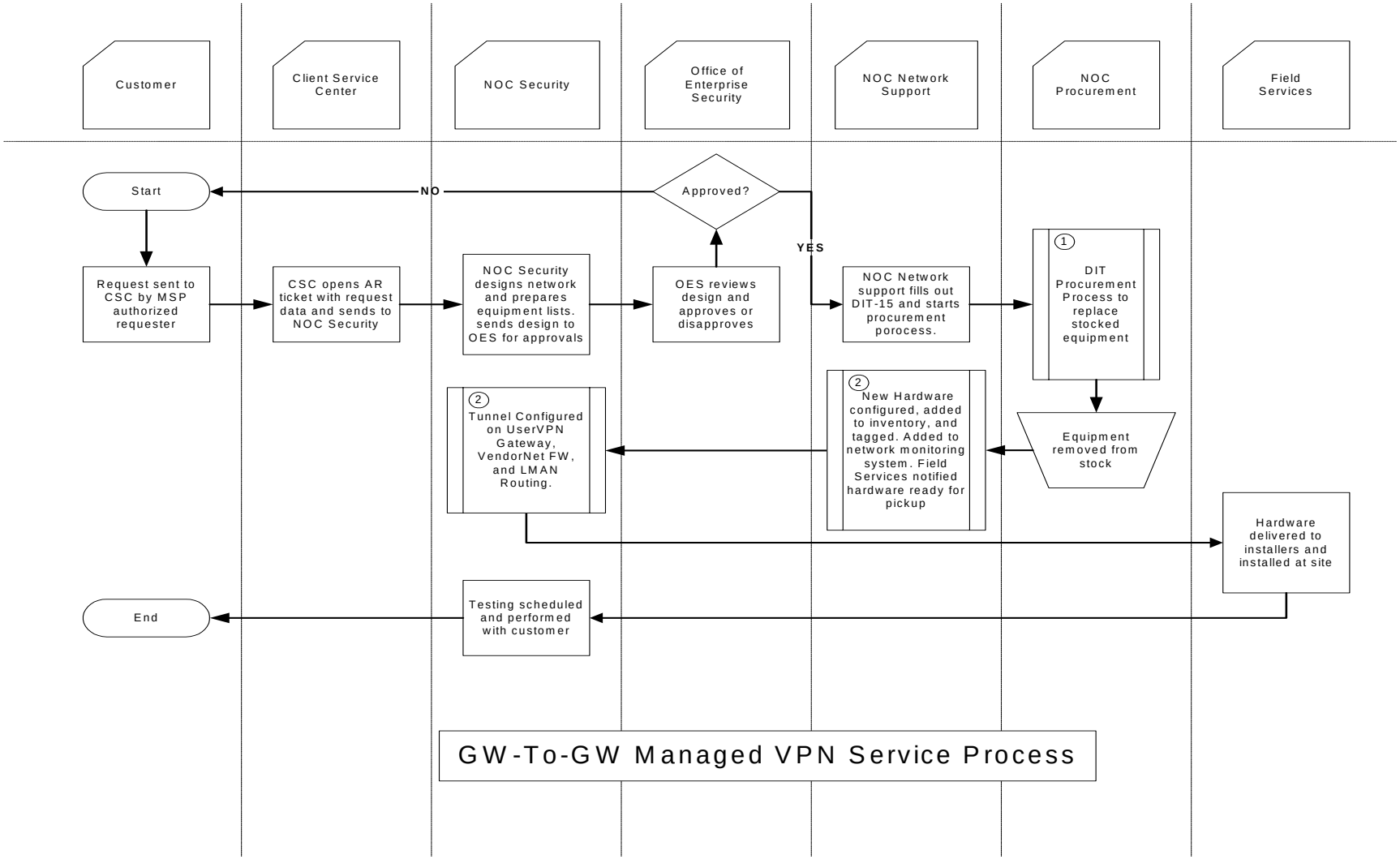
- Traffic within the VPN tunnel is 3DES encrypted and is generally considered safe from *man in the middle* attacks.
- Data transfer speeds are normally limited by the speed of the Internet connection at the slowest end.
- The customer ISP is the responsibility of the customer. DIT does not manage or recommend broadband providers for VPN access
- The ISP must be able to provide a single static IP address for the customer VPN gateway's external interface.
- SecurID and separate authentication to SoM is not required with GW-to-GW connections
- All hardware and software is included in the fee for User GW-to-GW. Network monitoring is also included. No hardware or software is provided for Vendor GW-to-GW and the Vendor is responsible for all setup/configuration on their end of the VPN tunnel.

Service costs

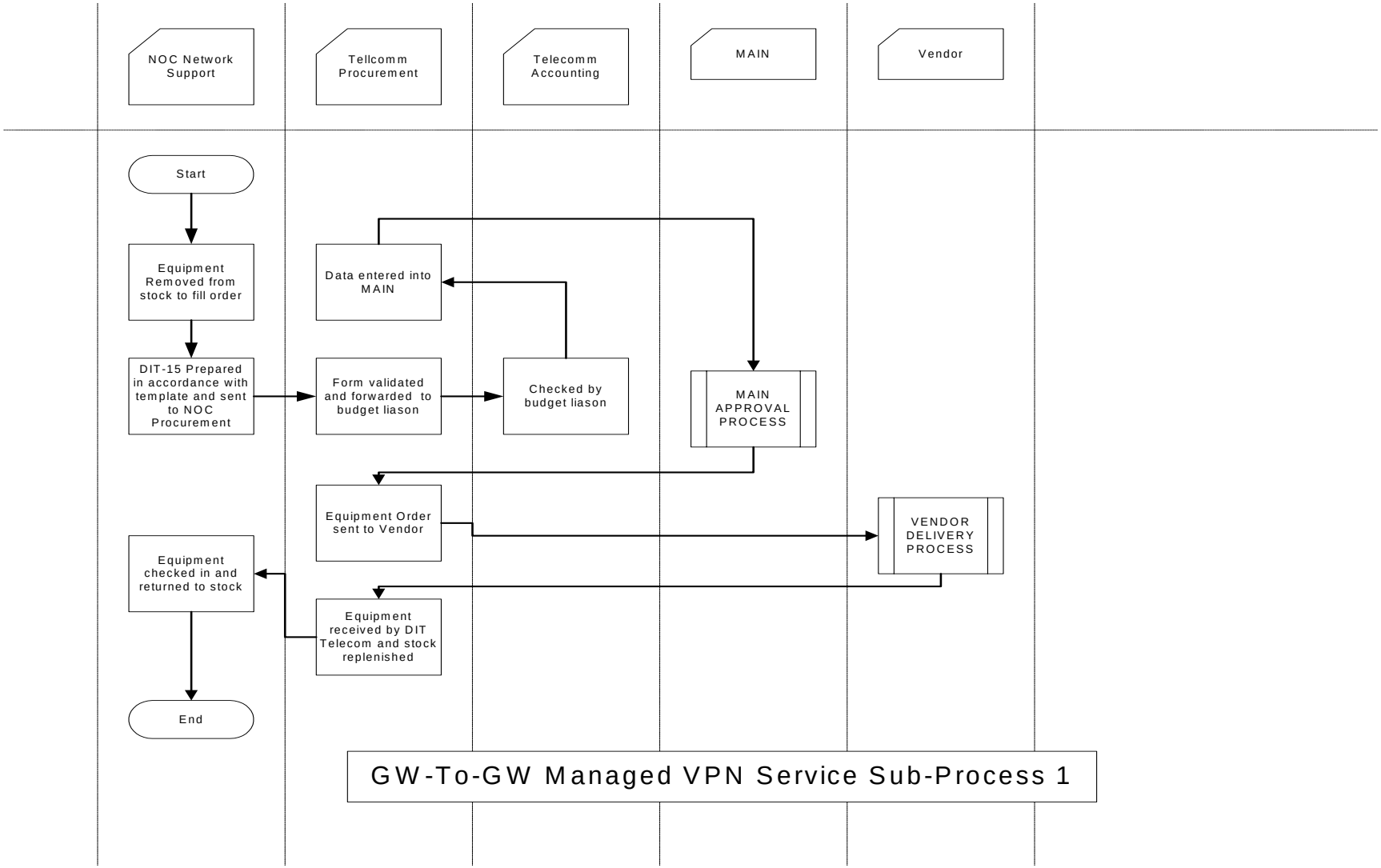
- Managed User Gateway-to-Gateway VPN
  - Setup fee $300.00
  - Monthly fee $258.00
- Unmanaged Vendor Gateway-to-Gateway VPN
  - Setup fee $300.00
  - Monthly fee $129
- There is no minimum service length but the Setup fee will be charged to re-enable a cancelled tunnel

Process Diagrams

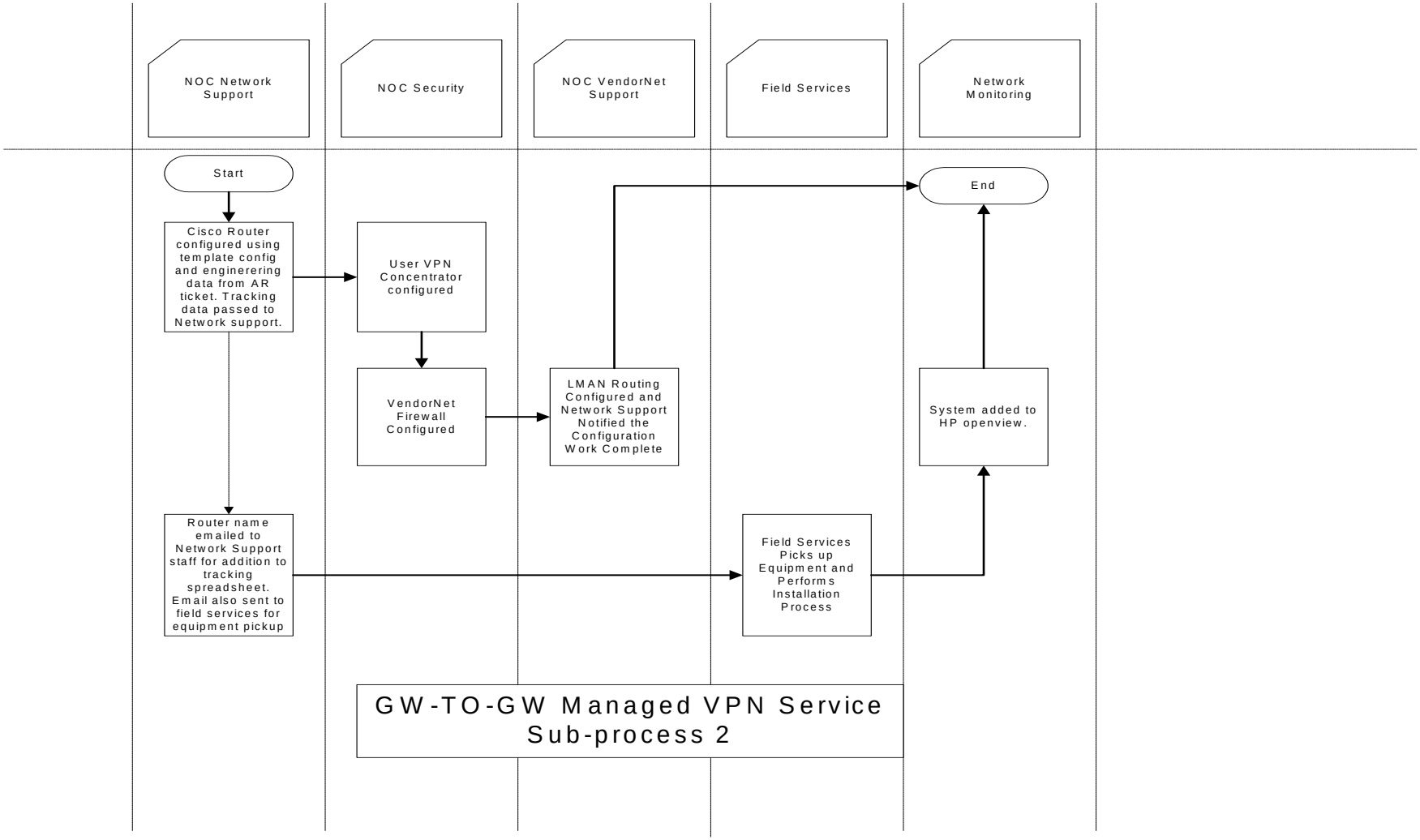
The following pages contain "swim lane" process diagrams that detail the workflow for constructing a GW-to-GW VPN service.



Overall Process Flow



Financial Process Flow



Hardware Configuration/Installation Flow

Step-By-Step Procedures

High Level Overview

The following pages contain step-by-step procedures for technicians configuring this service. This first table is intended as a high level guide for people already familiar with the tasks and can be used as a checklist.

Step	Task	Outcome	POC	Time
1	DIT-51 requesting new service is received by CSC	New helpdesk case is generated and sent to NOC Security with DIT-51 attached	CSC	1-2 hours
2	NOC Security reviews request and determines requirements	Updated ticket with design considerations is forwarded to OES	NOC Security team	1-2 days
3	OES approves/disapproves design	Approved ticket sent to NOC Network Security. If ticket is not approved it will be sent back to NOC security for redesign and may add time to process	OES	3-5 days
4	NOC Network support pulls hardware from stock and adds to tracking database, Tags equipment for deployment, configures router and switch for deployment, and adds new router to network monitoring environment	Updated ticket with configuration information sent to NOC Security	NOC Network Support	1-2 days
5	NOC Security team configures VPN concentrator, VendorNet Firewall, and VendorNet routes added for distant end	Updated ticket sent to Field services with notification of system ready for installation.	NOC Security	2-4 days
6	Field Services picks up equipment and installs at customer site. Configures customer LAN devices for use with new network	Service delivered to client. Updated ticket sent to NOC security for testing	Field Services	7-21 days
7	NOC Security contacts customer and tests service	Service delivered and tested	NOC Security	1 day

Equipment Procurement Process

Step	Task	Outcome	POC	Time
1	**The following codes are to be used to order stock for GW-to-GW rated services** **Remote Access Index and PCA codes** **These code are used by Telephone Service Center to bill back the customer** **Gateway to Gateway Vendor VPN** Group code = T137 Gateway-Gateway Vendor VPN Item code = RGWVVPN Gateway-Gateway Vendor VPN **Gateway to Gateway State User VPN** Group code = T136 Gateway-Gateway State User VPN Item code = RGWSUVPN Gateway-Gateway State User VPN	DIT pays for equipment to support rated service Customer is charged for service	Lisa Morison	

Systems Configurations

VPN Concentrators

Step	Task	Outcome	POC	Time
1	Open VPN management interface at ***"Removed in public version"*** and login	Presented with VPN concentrator main menu	NOC Security	1 Hour total
2	Browse to **Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN** and Click **Add**	Presented with LAN-to-LAN configuration screen		
3	Enter a name for the new tunnel in the format **AgencyOfficeCity** for User GW-to-GW example	Name entered into field		

	DITTelcomLansing or **CompanyToAgencyForApplication** for Vendor GW-to-GW example **AcmeToDITForRemedy**			
4	In the Peers field type the IP address of the Client Gateway device that was provided by the ISP Example **235.154.203.112**	IP Address entered into field		
5	In the pre-shared secret field type the 8 digit pre-share for GW-to-GW connections Example **Hs3F45a1**	Secret entered into field		
6	In the IKE Proposal field choose appropriate IKE proposal for the tunnel	Field info chosen		
7	In the Local Network section make the following selections Network List **Use IP Address/Mask Below** IP Address **0.0.0.0 (For User) or IP address, address range, or Network list name (for Vendor)** Wildcard Mask **255.255.255.255 (User) or appropriate mask for vendor tunnel (Vendor)**	Protected network fields populated		
8	In the Remote Network section make the following selections Network List **IP Network provided in ticket i.e. 10.125.15.0** Wildcard Mask **Reverse IP Subnet Mask provided in ticket i.e. 0.0.0.255**	Protected network fields populated		
9	Click the **Apply** button	You are presented with an informational screen that informs you of the new security associations, group, and filters that have been applied		
10	Click **OK**	You are returned to the LAN-to-LAN connections screen		

11	In the top right corner of the screen you will see a **"Save Needed"** Icon. Click it	A popup window will appear with the words "**Save Successful"** and an **OK** button.		
12	Click **OK**	The new GW-to-GW tunnel with the name given in step 3 is now listed.		END

Client Gateways for User GW-to-GW (1700 access routers)

Step	Task	Outcome	POC	Time
1	Connect the router up to a terminal via the console port and configure a terminal package for 8N1 @ 9600 BPS. Login to the router and get into enable mode and then configuration mode	yourname# yourname(config)#	Network Support	1.5 Hours
2	Copy the configuration from attachment 2 of this document into a text editor such as notepad and make the modifications at the highlighted areas.	Configuration complete in notepad		
3	Select **Edit | Select all** from the top line menu in notepad then select **Edit | Copy**	Configuration copied into system clipboard		
4	Go back to HyperTerminal and right click near the yourname(config)# prompt and select **Paste to Host**	Configuration is sent to router one line at a time and you are returned to the **RouterName#** prompt		
6	Type **wri mem** and hit enter	Building configuration... [OK] testrouter#		
7	Power down and repackage router for delivery			END

VendorNet Firewalls

Step	Task	Outcome	POC	Time

1	Log into VendorNet Firewall via GUI client.	Firewall administration screen.		0.5 Hrs
2	Create source object for gateway if not already there.	Source object created.		
3	Create destination object if not already there.	Destination object created.		
4	Place objects in an existing rule if appropriate.	Rule modified.		
5	Create new rule if necessary.	Rule creation.		
6	Push policy to firewall to update the rule base.	Allows acceptance of modified or new rule by firewall.		
7	Insure that a route exist for the source IP in the firewall Routing table.	Route for default gateway back to source IP.		END

LMAN Routing

Step	Task	Outcome	POC	Time
1	Add static routes pointing the "Assigned LMAN Private Address Space" to the VendorNet Firewall(s) in the Master LMAN Routing Distribution routers	"Assigned LMAN Private Address Space" will egress LMAN to VendorNet		

Network Monitoring

Step	Task	Outcome	POC	Time
1	Add trap destination to router configuration with the IP of ***"Removed in public version"***	traps (syslogs, etc.) will be sent to HPOV for storage & reports	Network Monitoring	
2	Put default LMAN community string in router configuration	Allows HPOV to snmp to router to collect information		
3	Give us a list of the hostname & IPs of all	So we are able to monitor these routers & report their		

	devices	status to the CSC		
4	If necessary, allow access to these routers via icmp & snmp through any firewalls	So we are able to monitor these routers & report their status to the CSC		
5	Include HPOV ***"Removed in public version"*** in any ACLS	So we are able to monitor these routers & report their status to the CSC		

Hardware Inventory/Check in/Restock

Step	Task	Outcome	POC	Time
1	Type up DIT-15, send for approval signatures, accounting and order with SBC	Orders Equipment	NOC Network Support	20 Mins
2	Order is received, tagged and serial number recorded	Have stock		30 Mins
3	Retrieve stock from storage for configuration for site	Sent to site for installation		1 Hour
4	Type up DIT-15 for replacement equipment	Replenish Equipment		20 Mins

Site hardware installation for User GW-to-GW

Step	Task	Outcome	POC	Time
1	Perform a site visit to determine installation location and backboard requirements**.**	Detailed site plan for installation.	DIT Field Services	2 Days
2	A determination of the location of the VPN and Cable Modem equipment on backboard	Detailed backboard drawing produced		2 hours
3	Install lockable rack on backboard			1 hour
4	Install Modem, Router, and Switch			1 hour
5	Router Eth Ch 1 is connected to the cable modem, with a crossover cable.			5 minutes
6	Router Eth Ch 2 is connected to port 1 of the switch.			5 minutes

7	Connection from the switch to the clients patch panel would then be made with client supplied patch cables of the appropriate length			5 minutes
8	Test connection	Ticket Closed		END

Attachments

Attachment 1 - Example of DIT-51 request for remote access service

REMOTE ACCESS SERVICE REQUEST
Michigan Department of Information Technology

SECTION I – EMPLOYEE INFORMATION (CARD HOLDER)

1. Last Name	First Name	Init	2. Email Address
Doe	John	Q	doej@michigan.gov

3. Agency / Office / Division / Section / Unit: DIT/Telecommunications/NOC/Security

4. Business Street Address	5. Business City	State	Zip
123 West East St	Anywhere	MI	55555

6. Business Phone No.	Extension	7. Last 4 digits SS#	8. Birth Date *(month & day only-mmdd)*
(517)555-1212	1234		

9. State User Access
☐ State Employee
☐ Contractor / Company Name

10. Vendor Access
Vendor Company Name

SECTION II – SERVICE REQUESTED

1. Access Requested ☐ **SecurID Only**
☐ Dial-in ☐ VPN **If checked, VPN Group** _____ ☐ Both
X User GW-toGW - RGWSUVPN X Vendor GW-to-GW - RGWVVPN Labor Units ____ Code NLROAM

2. Firewall Access requested: Destination, TCP/IP Port
ISP Provided static address (User)or Peer GW address (Vendor)= XXX.XXX.XXX.XXX
ISP Provided default GW address (User only) = 255.255.255.XXX
SoM Provided private address space (User space provided by NOC) or Vendor protected network space (must be public address space i.e. Not 10.X.X.X or 192.168.X.X) provided by the vendor
Technical Point of contact(POC)at the distant end (Vendor)site POC (User) Name, Phone, Email

3. Change Access Type – Existing assigned token only

Add:	☐ Dial-in/ROAM	☐ VPN
Remove:	☐ Dial-in/ROAM	☐ VPN

4. Reissue – No Division Approval required for reissue
☐ Reissue

5. Cancel Token *(Check appropriate reason)* ☐ Lost ☐ Expired ☐ No longer needed ☐ Defective / Damaged

6. Token Serial # / Tunnel Name

SECTION III – DIVISION APPROVAL

1. Division Approver Name	2. Telephone Number
Ms Lottsa Cash	(517) 555-1111

3. Division Approver Signature — Date

SECTION IV – DEPARTMENT SECURITY ADMINISTRATOR APPROVAL

1. Security Administrator Name	2. Telephone Number
Ima Watchenya	(517) 555-9999

3. Security Administrator Approval Signature — Date

SECTION V – BILLING INFORMATION

1a. Ag Code	1b. Index	1c. PCA	1d. COBJ	1e. AOBJ	1f. Project #	1g. Prj Ph	1h. Grant #	1i. Grt Ph	1j. Ag 1	1k. Ag 2	1l. Ag 3
XXX	XXXX	XXXXX									

When the above information has been completed, fax this form to (517) 241-8016.

HELP DESK USE ONLY

1. Ticket Number	2. Assigned by:	3. Date

NOC SECURITY USE ONLY – NEW CARD

4. Token Serial #	5. SecurID Administrator Signature *(Required)*	6. Start Date

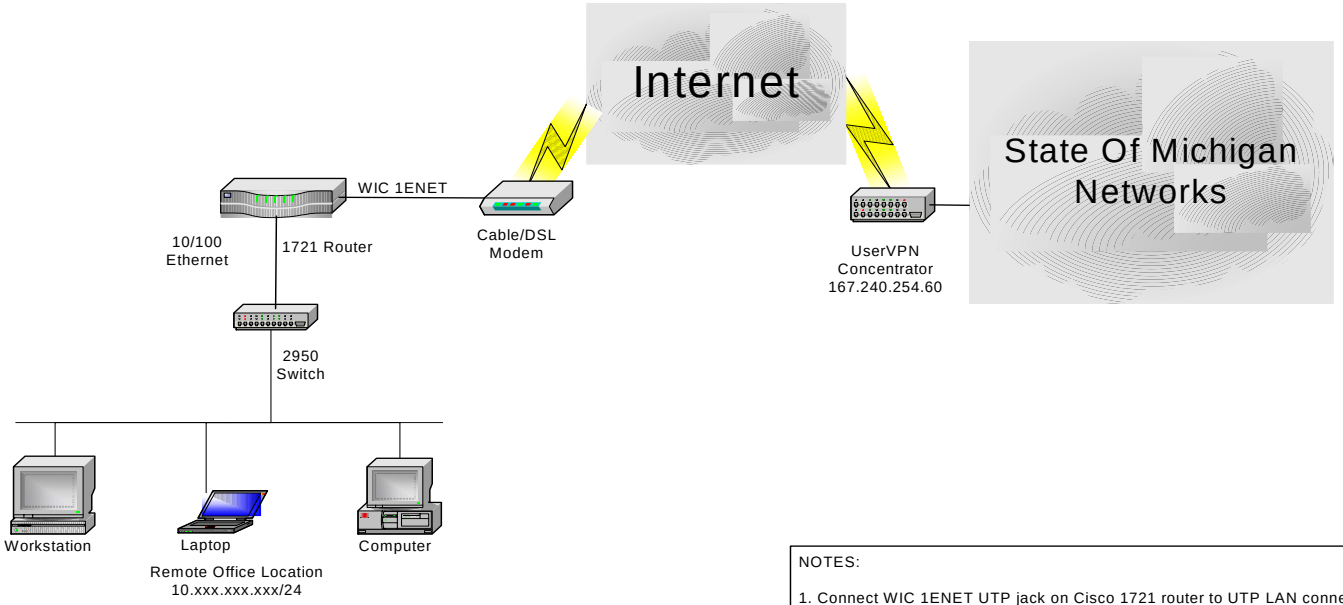
NOC SECURITY USE ONLY – CANCEL CARD *Note: DIT will continue to charge Agency until card is returned or reported lost*

7. Token Received by Signature	8. End Date

Attachment 2 – Cisco 1721 router configuration template

"Removed in public version"

Attachment 3 – Functional wiring diagram for User GW-to-GW remote location



NOTES:

1. Connect WIC 1ENET UTP jack on Cisco 1721 router to UTP LAN connecton on cable modem or DSL modem provided by ISP

2. Connect 10/100 Ethernet UTP jack on Cisco 1721 router to port 1 on Cisco Catalyst 2950 series switch

3. Connect site wiring to remaining ports on Cisco 2950 series switch

4. Insure that all PC's that are going to be connected to the Remote Office Location LAN are set for DHCP auto-configuration

Attachment 4 – DIT-0051 Process flow diagram